

1 CLAIMS

2
3 1. A system comprising:

4 a set of filters;

5 a mapping of virtual addresses to network addresses; and

6 a controller, coupled to the set of filters and the mapping, to,

7 access, upon receipt of a data packet requested to be sent from a
8 computing device to a target device via a network, the set of filters and
9 determine whether the data packet can be sent to the target device based on
10 whether the computing device is allowed to communicate with the target
11 device,

12 replace, based on the mapping, the target address in the data packet
13 with a corresponding target network address; and

14 forward the data packet to the target device at the target network
15 address if it is determined the data packet can be sent to the target device.
16

17 2. A system as recited in claim 1, wherein the controller is further to
18 prevent the computing device from modifying any of the filters in the set of filters.
19

20 3. A system as recited in claim 1, wherein the computing device
21 includes the system.
22
23
24
25

4. A system as recited in claim 1, wherein the controller is to make the computing device aware of the virtual addresses in the mapping but to hide the network addresses in the mapping from the computing device.

5. A system as recited in claim 1, wherein the controller is further to allow the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels.

6. A system as recited in 5, further comprising allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device.

7. A method comprising:

- maintaining, at a computing device, a set of filters that restrict the ability of the computing device to communicate with other computing devices;
- allowing the set of filters to be modified from a remote device; and
- preventing the computing device from modifying the set of filters.

8. A method as recited in claim 7, wherein restriction of the ability of the computing device to communicate with other computing devices comprises restricting the computing device from transmitting data packets to one or more other computing devices.

9. A method as recited in claim 7, wherein modification of the set of filters includes one or more of: adding a new filter to the set of filters, deleting a filter from the set of filters, and changing one or more parameters of a filter in the set of filters.

10. A method as recited in claim 7, wherein one or more filters in the set of filters restrict one or more of the transmission of data packets of a particular type from the computing device and reception of data packets of a particular type at the computing device.

11. A method as recited in claim 7, wherein one or more filters in the set of filters restrict one or more of the transmission of Internet Protocol (IP) data packets from the computing device and reception of IP data packets at the computing device based on one or more of: a source address, a destination IP address, a source port, a destination port, and a protocol.

12. A method as recited in claim 7, wherein one or more filters in the set of filters identifies that a data packet targeting a particular address can be transmitted from the computing device to the addressed device, and further identifies a new address that the particular address from the data packet is to be changed to prior to being communicated to the addressed device.

1 18. A method as recited in claim 7, wherein the set of filters restrict the
2 ability of the computing device to communicate with other computing devices on a
3 per-data packet basis, wherein each filter includes a plurality of filter parameters,
4 and wherein each filter parameter includes a filter value and a mask value
5 indicating which portions of the filter value must match a corresponding parameter
6 in a data packet for the data packet to satisfy the filter.

7
8 ✓19. One or more computer-readable memories containing a computer
9 program that is executable by a processor to perform the method recited in claim
10 7.

11
12 ✓20. A network mediator comprising:

13 a set of filters; and

14 a controller, coupled to the set of filters, to,

15 access, upon receipt of a data packet requested to be sent from a
16 computing device to a target device via a network, the set of filters and
17 determine whether the data packet can be sent to the target device based on
18 whether the computing device is allowed to communicate with the target
19 device, and

20 preventing the computing device from modifying any of the filters in
21 the set of filters.
22
23
24
25

1 **21.** A network mediator as recited in claim 20, wherein the controller is
2 further to access, upon receipt of another data packet from another target device
3 via the network, the set of filters and determine whether the data packet can be
4 received at the computing device based on whether the computing device is
5 allowed to receive communications from the other target device.

6
7 **22.** A network mediator as recited in claim 20, wherein the modifying of
8 a filter includes one or more of: adding a new filter to the set of filters, deleting a
9 filter from the set of filters, and changing one or more parameters of a filter in the
10 set of filters.

11
12 **23.** A network mediator as recited in claim 20, wherein the network
13 mediator is coupled to the computing device.

14
15 **24.** A network mediator as recited in claim 20, wherein the computing
16 device includes the network mediator.

17
18 **25.** A network mediator as recited in claim 20, wherein each filter in the
19 set of filters includes a plurality of filter parameters, and wherein each filter
20 parameter includes a filter value and a mask value indicating which portions of the
21 filter value must match a corresponding parameter in the data packet for the data
22 packet to satisfy the filter.

1 26. A network mediator as recited in claim 25, wherein the controller is
2 to allow the data packet to be forwarded to the target device if the data packet
3 satisfies the filter.

4
5 27. A network mediator as recited in claim 25, wherein the controller is
6 to prevent the data packet from being forwarded to the target device if the data
7 packet satisfies the filter.

8
9 ✓28. A method comprising:
10 maintaining a set of filters that restrict the ability of a computing device to
11 communicate with other computing devices;
12 allowing multiple remote computing devices, each corresponding to a
13 different managerial level, to modify the set of filters; and
14 preventing a lower managerial level device from modifying the set of filters
15 in a manner that would result in a violation of a filter added by a higher
16 managerial level device.

17
18 29. A method as recited in claim 28, wherein the preventing comprises:
19 receiving a request from the lower managerial level device to modify the
20 set of filters;
21 determining whether the requested modification would result in a violation
22 of a filter previously added to the set of filters by the higher managerial device;
23 and
24 performing the requested modification if the requested modification would
25 not result in a violation, and otherwise not performing the requested modification.

1 ✓ 35. One or more computer-readable media having stored thereon a
2 computer program to implement a multiple-level filter administration scheme and
3 including a plurality of instructions that, when executed by one or more
4 processors, causes the one or more processors to perform acts including:

5 allowing a first computing device operating at a first of the multiple levels
6 to modify a set of filters corresponding to a filtered device; and

7 allowing a second computing device operating at a second of the multiple
8 levels to modify the set of filters only if the modification is at least as restrictive as
9 the filters imposed by the first computing device.

10
11 36. One or more computer-readable media as recited in claim 35,
12 wherein the plurality of instructions further include instructions that, when
13 executed by the one or more processors, causes the one or more processors to
14 perform acts including allowing the first computing device to remove a filter from
15 the set of filters imposed by the first computing device but not allowing the second
16 computing device to remove the filter.

17
18 37. One or more computer-readable media as recited in claim 35,
19 wherein modifying the set of filters comprises one or more of: adding a new filter
20 to the set of filters, removing a filter from the set of filters, and changing
21 parameters of a filter in the set of filters.

1 **38.** One or more computer-readable media as recited in claim 35,
2 wherein the plurality of instructions further include instructions that, when
3 executed by the one or more processors, causes the one or more processors to
4 perform acts including preventing the filtered device from modifying the set of
5 filters.

6
7 **39.** A method comprising:
8 maintaining an association of virtual addresses and corresponding network
9 addresses;
10 making a computing device aware of the virtual addresses;
11 hiding the network addresses from the computing device;
12 receiving, from the computing device, a data packet intended for a target
13 computing device corresponding to a target virtual address;
14 replacing, based on the target virtual address, the target virtual address with
15 the corresponding target network address; and
16 forwarding the data packet to the target computing device at the target
17 network address.

18
19 **40.** A method as recited in claim 39, wherein the replacing comprises
20 performing the replacing transparent to the computing device.

21
22 **41.** A method as recited in claim 39, further comprising:
23 receiving, from a source device, another data packet that is intended for the
24 computing device, wherein the other data packet includes a network address of the
25 source device; and

1 replacing, based on the network address of the source device, the network
2 address of the source device with a corresponding virtual address.

3
4 **42.** A method as recited in claim 39, further comprising:
5 maintaining, at the computing device, a set of filters that further restrict the
6 ability of the computing device to communicate with other computing devices;
7 allowing the set of filters to be modified from a remote device; and
8 preventing the computing device from modifying the set of filters.

9
10 **43.** A method as recited in claim 39, further comprising:
11 maintaining a set of filters that restrict the ability of the computing device
12 to communicate with other computing devices;
13 allowing multiple remote computing devices, each corresponding to a
14 different managerial level, to modify the set of filters; and
15 preventing a lower managerial level device from modifying the set of filters
16 in a manner that would result in a violation of a filter added by a higher
17 managerial level device.

18
19 **44.** One or more computer-readable memories containing a computer
20 program that is executable by a processor to perform the method recited in claim
21 39.

22
23 ✓ **45.** A network mediator comprising:
24 a mapping of virtual addresses to network addresses; and
25 a controller, coupled to the mapping, to,

1 make a corresponding computing device aware of the virtual
2 addresses,

3 hide the network addresses from the computing device,

4 receive, from the computing device, a data packet intended for a
5 target computing device corresponding to a target virtual address,

6 replace, based on the target virtual address, the target virtual address
7 with the corresponding target network address, and

8 forward the data packet to the target computing device at the target
9 network address.

10
11 **46.** A network mediator as recited in claim 45, wherein the network
12 mediator is communicatively coupled to the computing device.

13
14 **47.** A network mediator as recited in claim 45, wherein the computing
15 device includes the network mediator.

16
17 **48.** A network mediator as recited in claim 45, further comprising:
18 a set of filters that further restrict the ability of the computing device to
19 communicate with other computing devices; and
20 wherein the controller is further to,

21 allow the set of filters to be modified from a remote device, and

22 prevent the computing device from modifying the set of filters.
23
24
25